PII Breach Management and Risk Assessment

Privacy Officer Roles

- Oversight
- Compliance
- Breach Management

What is a Breach?

The actual or possible loss of control, unauthorized disclosure, or unauthorized access of personally identifiable information (PII) where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected.

Source: DoD 5400.11-R, "DoD Privacy Program", May 14, 2007

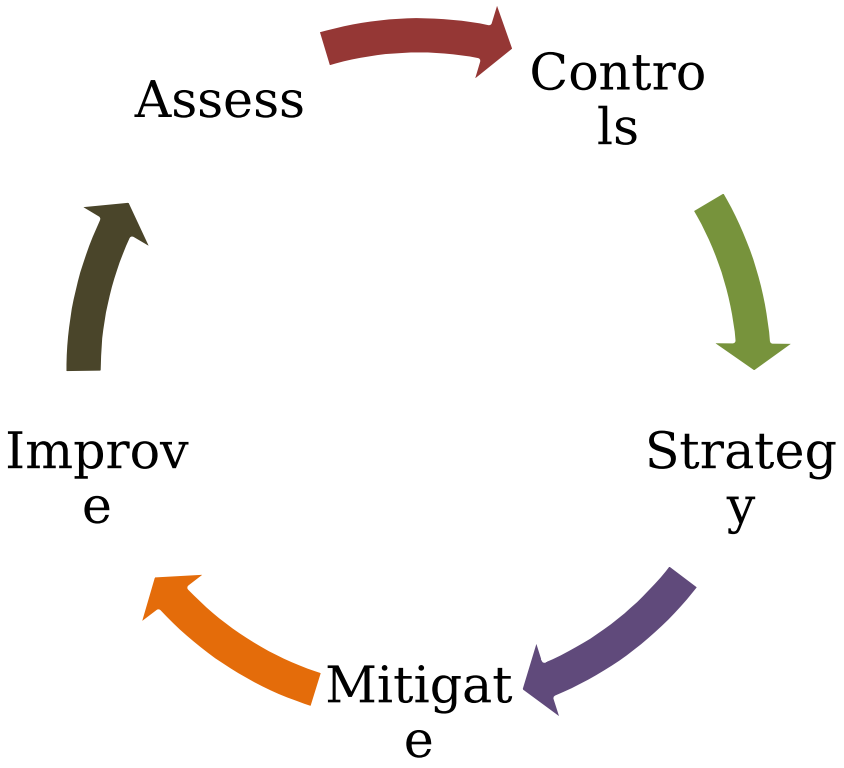
Has a Breach Occurred?

- Basic questions for establishing a breach
  - Did you lose it?
  - Did someone steal it?
  - Was it compromised?

Assessing Breach Risk

- Evaluate the risk to the individual and to the organization
  - The greater the sensitivity of the data, the greater the risk of harm to individual
  - Level of risk depends on manner of the actual breach and the nature of the data involved
- Determination to notify should only be made after this assessment (risk of harm and level of risk as result from loss, theft, compromise of data) is complete

Risk Management Cycle



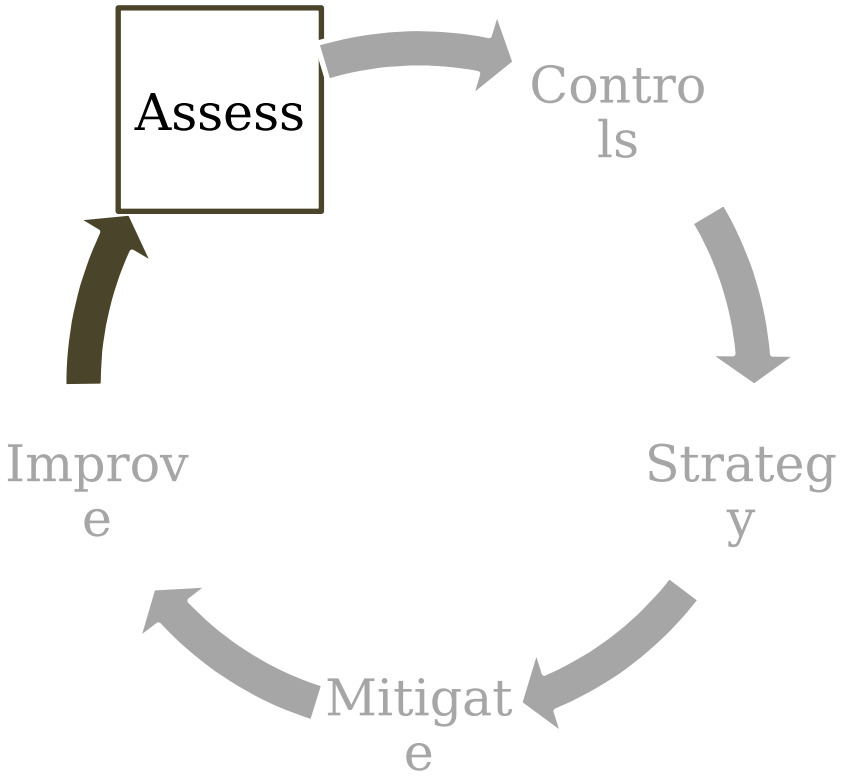
Pros

- Continuous improvement
- Adapts to any environment
- “Grows” with changes
- More reliable

Cons

- Time intensive to establish
- Needs constant monitoring to be effective

Assess the Environment

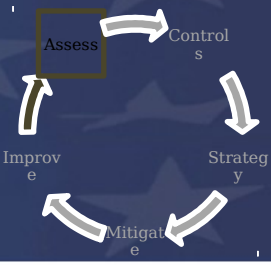


- Inventory assets
- Inventory systems
- Identify vulnerabilities and threats

Know the Facts

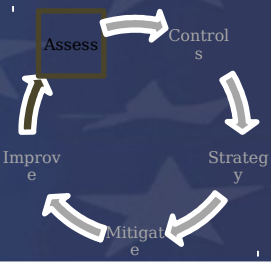
- Whose PII was involved?
- What PII was involved?
- Where was the PII housed?
- How was the PII compromised?
- When was the PII compromised?

Vulnerability



- Any weakness of an information system, system security procedures, internal controls, or implementation that can be exploited
- Types of vulnerabilitie
  - Technical
  - Physical
  - Administrative

Threat

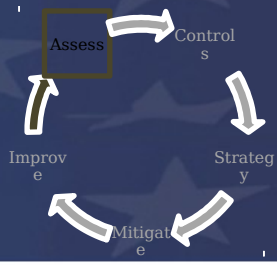


- Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service
- Types of threats
  - Natural
  - Man-made
  - Environmental

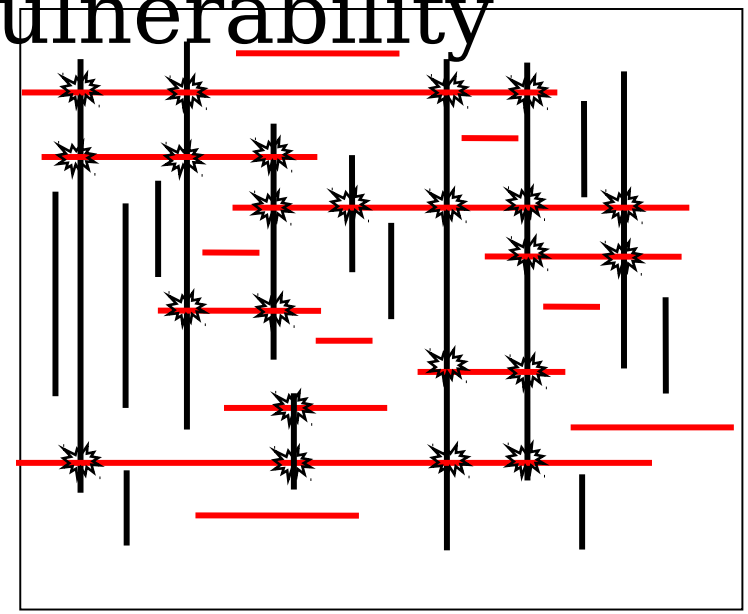
Power Failure

Arson

Risk



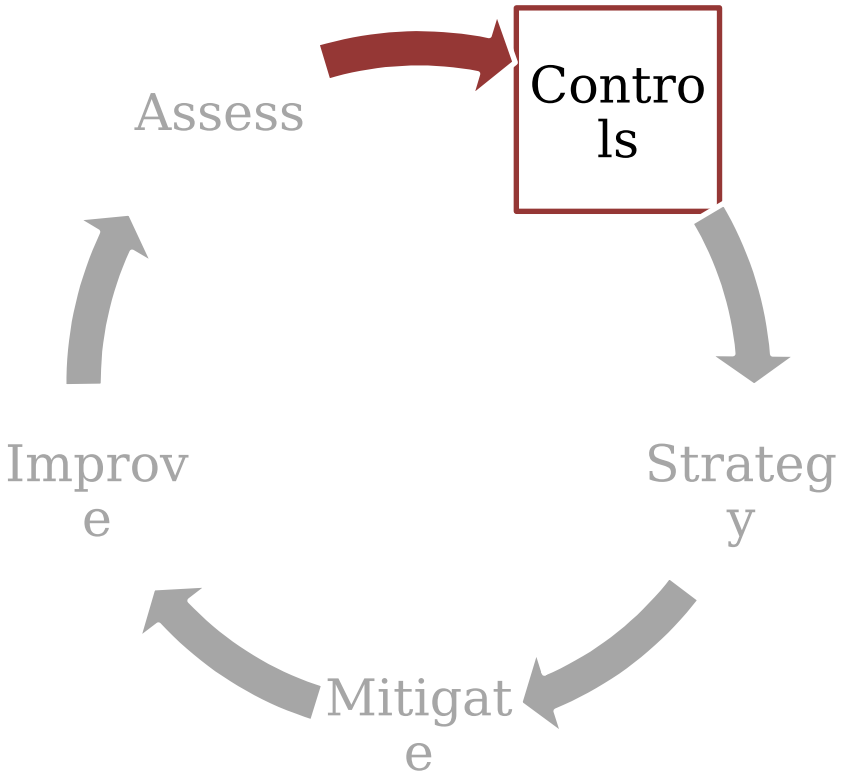
- Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability



Key:

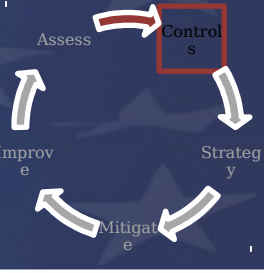
- Threats
- Vulnerabilities
- Risks

Establish and Test Controls

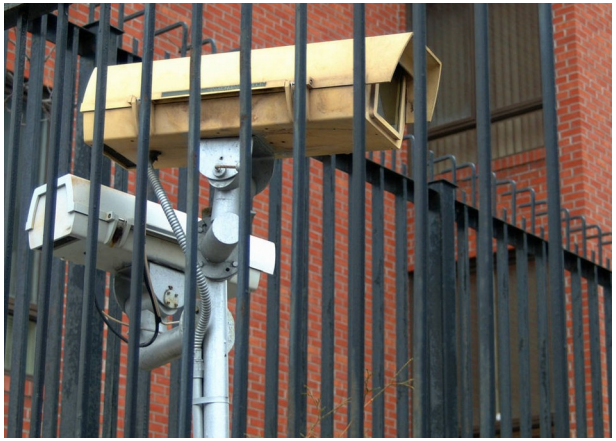


- Inventory policies
- Inventory processes and procedures
- Compare controls to identify risks

Safeguards



- A protection included to counteract a known or expected condition
- An incorporated countermeasure or set of countermeasures



Source: DoDI 8500.02

Administrative Controls

- Policies
- Procedures
- Training
  - Orientation
  - Specialized
  - Management

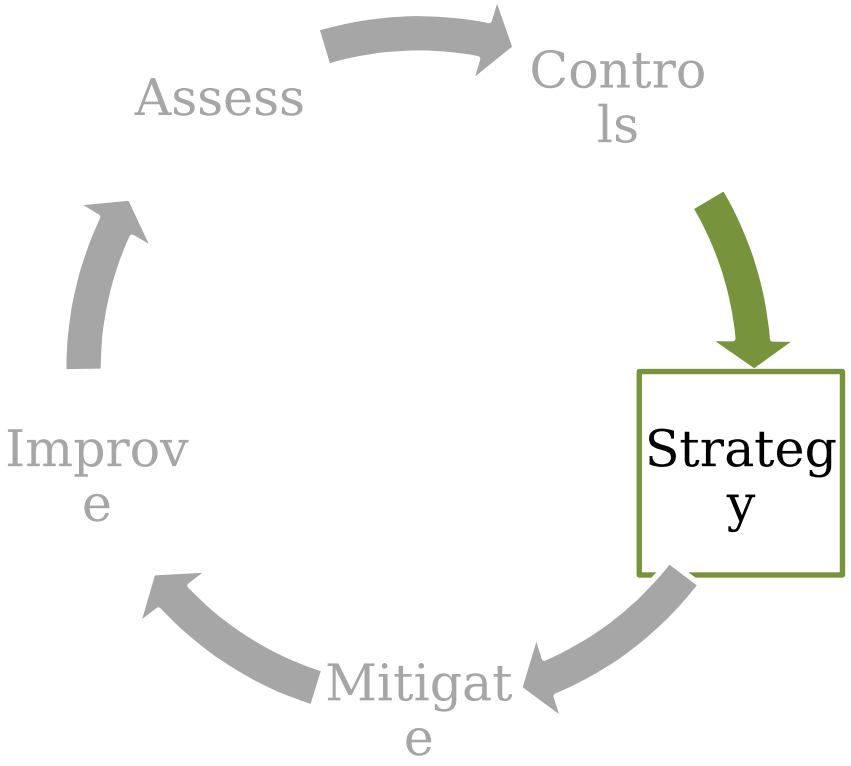
Technical Controls

- Ensure laptops are CAC enabled and have encryption software
- Encrypt PII when electronically transmitted
- Ensure systems have appropriate permissions settings

Physical Controls

- Develop access procedures
- Safeguard mobile devices
- Store paper records in locked cabinets
- Ensure use of coversheets on documents containing PII

Define the Mitigation Strategy



- Analyze impact of each risk
- Prioritize the risks
- Determine mitigation plan

Factors to Analyze Breach Risk

- How the loss occurred
- Nature of data elements breached and number of individuals affected
- Ability and likelihood that the information is accessible and useful
- Evidence and likelihood a breach may lead to harm
- Ability of the agency to mitigate the risk of harm

Definitions of Likelihood of Risk

High

- The nature of the attack and data indicate that motivation is criminal intent.
- The security of the data and controls to minimize the likelihood of a privacy violation are ineffective.
- Countermeasures are recommended to mitigate these risks and should be implemented as soon as possible.

Medium

- The nature of the attack and data indicate that the motivation could be criminal intent.
- Controls are in place that may impede success.
- Countermeasure implementation should be planned in the near future.

Low

- The nature of the attack and data do not indicate criminal intent; security and controls are in place to prevent, or at least significantly impede the likelihood of a privacy violation.
- Countermeasure implementation will enhance security, but is less urgent than the above risks.

Assessing Risk and Harm to the Organization and Individuals:

Risk is a function of the probability or likelihood of a privacy violation and the resulting impact of that violation. To assign a risk score, assess the probability that the event (data breach) will occur, and then assess the impact or harm that may be caused to an individual and/or your organization's ability to achieve its mission.

Definitions of Impact Rating

High	Medium	Low
• Event may result in human death or serious injury or harm to the individual; • may result in high cost to the organization; or • may significantly violate, harm, or impede an organization's mission, reputation, or interest.	• Event may result in injury or harm to the individual; • may result in costs to the organization; or • may violate, harm, or impede an organization's mission, reputation, or interest.	• Event may result in the loss of some tangible organizational assets or resources; or • may noticeably affect an organization's mission, reputation, or interest.

Impact Rating:

The impact depends on the extent to which the breach posses a risk of identity theft or other substantial harm to an individual such as, embarrassment, inconvenience, unfairness, harm to reputation, or the potential for harassment or prejudice, particularly when health or financial benefits information is involved (5 U.S.C. 552a (e)(10)).

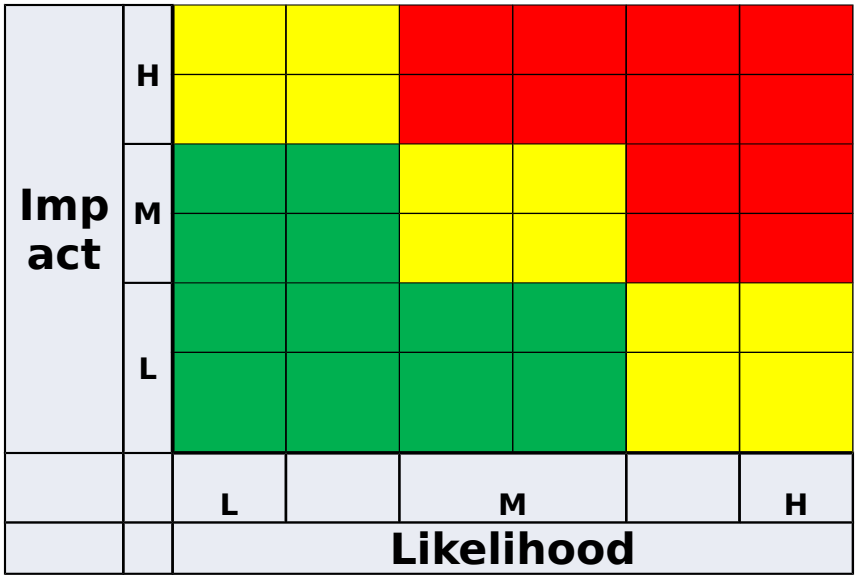
Organizational Risk Assessment Team

- General Counsel
- CIO Representative
- Public Affairs
- Inspector General
- Component Senior Official for Privacy

Others as needed

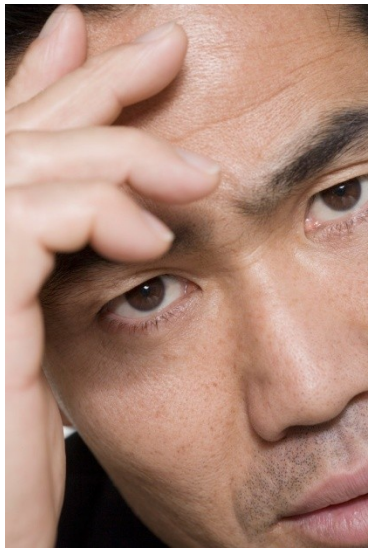
Risk Rating

- Administrative burden
- Cost of remediation
- Loss of public trust
- Legal liability



Assessing Harm to the Individual

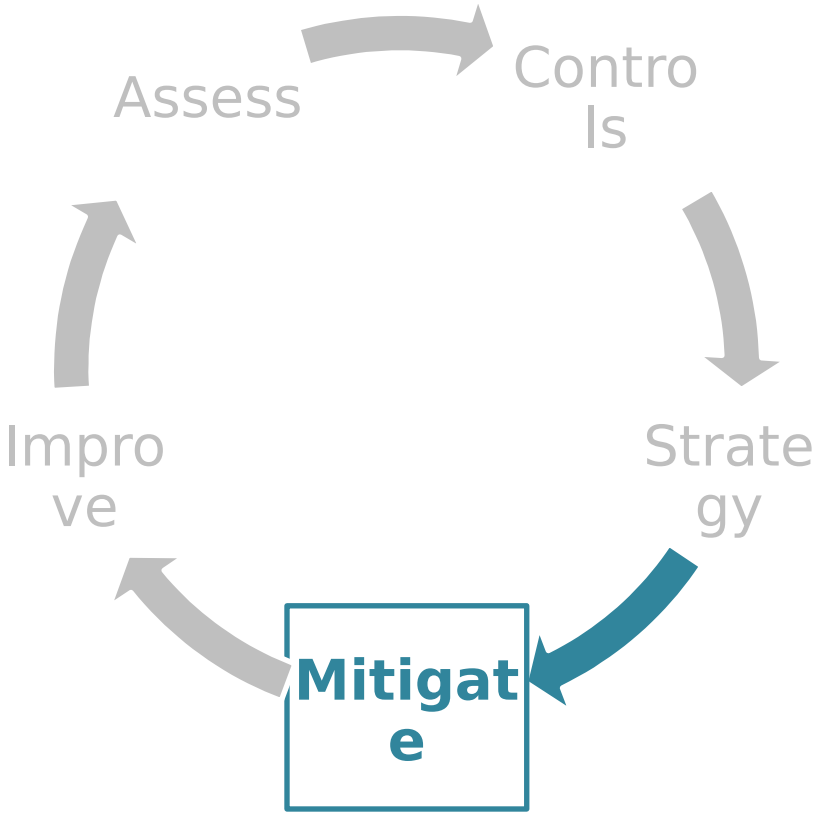
- What are the chances of significant harm to the individual?
- Harm includes:
  - Identity theft
  - Discrimination
  - Emotional distress
  - Inappropriate denial of benefits
  - Physical harm
  - Blackmail



Examples - Breach Risk Factors

Factors	Examples	
How the loss occurred	➢ Online system hacked ➢ Data was targeted ➢ Device was targeted	➢ Device was stolen ➢ Device lost
Nature of the data elements breached and number of individuals impacted	➢ Social Security Number ➢ Biometric record ➢ Financial account number ➢ PIN or security code for financial account ➢ Health data	➢ Birth date ➢ Government Issued Identification Number (driver's license, etc) ➢ Name ➢ Address ➢ Telephone number
The ability and likelihood of gaining access to the data	➢ Paper records or electronic records in a spreadsheet that is not password-protected	➢ Electronic records are only password-protected ➢ Electronic records are password-protected and encrypted
The ability to mitigate the risk of harm	➢ No recovery of data ➢ Partial recovery of data	➢ Recovery of data prior to use
Evidence and likelihood of data being used for identity theft or other harm	➢ Data published on the web ➢ Data accessed but no direct evidence of use	➢ No tangible evidence of data use

Mitigate Risks in the Environment



- Identification
- Eradication
- Containment
- Reporting
- Notification
- Mitigation
- Recovery
- Follow-up

Identification

- Involves examining all available information in order to determine if an event/breach has occurred
- Determine if the breach was a single instance or recurring event
- Action Steps
  - Analyze all available information
  - Confirm and classify the severity of the breach
  - Determine the appropriate plan of action
  - Acknowledge legal issues
  - Evaluate the circumstances and document details

Eradication

- Remove the cause of the breach and mitigate vulnerabilities pertaining to it
- If the cause of the breach cannot be removed, isolate the affected PII
- Effective eradication efforts include administrative and physical safeguards in addition to technical safeguards

Containment

- Implement short-term actions immediately to limit the scope and magnitude of a breach
- Determine the media of PII that may be affected—paper, electronic, or both
- Minimum Action Steps include:
  - Determine a course of action concerning the operational status of the compromised system and identify critical information affected by the breach
  - Follow existing local and higher authority guidance regarding any additional breach containment requirements

Reporting

- 1 hour to the United States Computer Emergency Readiness Team (US-CERT)
- 24 hours to Component Senior Official for Privacy (CSOP)
- 48 hours to Defense Privacy and Civil Liberties Office (DPCLO)
- 10 working days for individual notification

NOTE: If individual notification is delayed, inform DPCLO

Reporting

Component Report

Component Privacy Official submits breach report (initial and/or follow-up)

DPCLO Summary Report

DPCLO compiles reports and submits summary to DoD's Senior Agency Official for Privacy (SAOP)

Tracking

DPCLO enters report information into database to identify trends and ID issues

Mitigation of Harmful Effects

- Notify system owners of attempted breach
- Identify personnel who may be involved and ensure they are performing required duties to contain harmful effects
- Apply appropriate administrative safeguards, including reporting and analysis
- Apply appropriate physical safeguards, such as, controlling any affected PII and securing hardware
- Apply appropriate technical safeguards, such as blocking all exploited ports

Notification

If there is a *significant* chance that the individual can be *significantly* harmed by the breach, *notify* the individual.

It is your Component's responsibility to determine what is 'significant'.

Notification Requirements

- Head of DoD Component or senior level individual from the organization where breach occurred
- 1st class U.S. Mail
- Other means acceptable if more effective in reaching affected individuals
  - Email
  - Telephone (must be followed up in writing)
- Support services, including toll free number and website

Elements of Notification

- If the Component Privacy Office determines that notification is necessary, the following elements should be included:
  - A description of what specific data that was involved
  - Facts and circumstances surrounding the loss, theft, or compromise
  - A statement regarding if and how the data was protected (i.e., encryption)
  - Any mitigation support services implemented by the agency
  - Protective actions that are being taken or other actions the individual can take to protect themselves against future harm
  - Provide a point of contact for more information

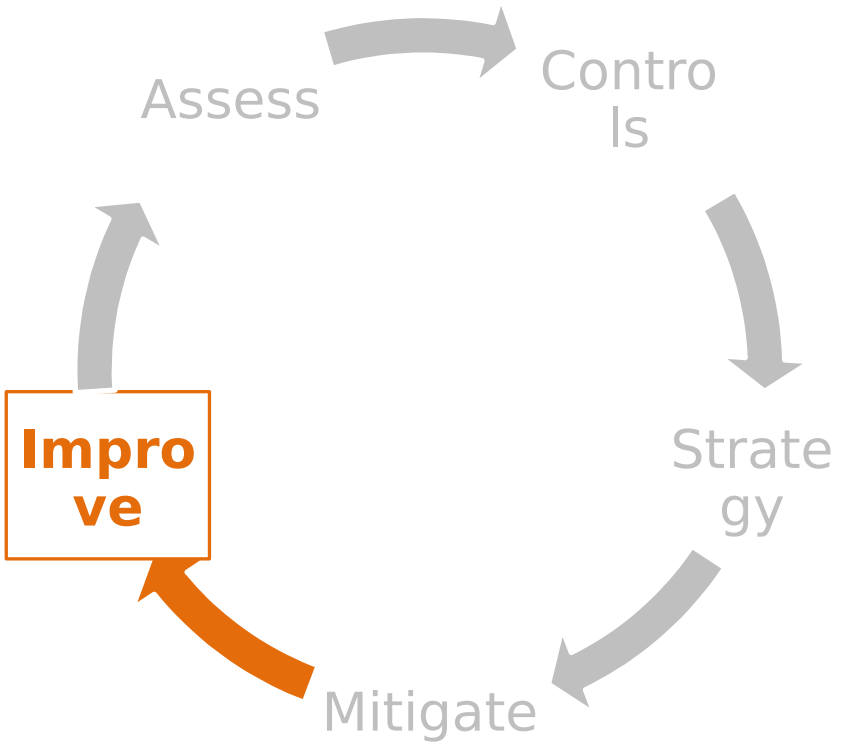
Recovery

- Execute the necessary changes to the environment and document recovery actions in the breach identification log
- Notify users of policy updates, new standard operating procedures and processes, and security upgrades that were implemented due to the breach

Follow-up

- Develop a lessons learned list, share with DoD personnel and with other DoD organizations, as applicable
- Establish new assessment procedures in order to identify or prevent similar breaches in the future
- Provide subsequent workforce training and awareness lessons, as necessary

Set a Pattern of Improvement



- Report findings
- Revise/rewrite policies and SOPs
- Continually monitor for new risks / guidance
- Update controls

Be Proactive

- Practice proactive risk management
  - Map how PII travels through the facility
  - Identify its location in transit and at rest
  - Keep a plan of action and updated policies and procedures